

Whitepaper

Eine eigenständige Proof-of-Work-Blockchain für selbst betriebene Nodes, Wallets und Solo-Mining.

Technische Ausgabe · 26. September 2026 · Deutsch

Netzwerk	Eigenes Mainnet · STP
Konsens	SHA-256d Proof of Work
Status	Laufendes Mainnet; unabhängiges Sicherheitsaudit ausstehend

Dieses Dokument beschreibt die gegenwärtig implementierten Regeln und beobachteten Freigabetests. Es verspricht weder einen Marktwert noch eine Börsennotierung. Für produktive Integrationen sind die Regeln anhand des veröffentlichten Quellcodes und einer eigenen Node zu prüfen.

1. Zusammenfassung

Stompi ist eine eigenständige Kryptowährung mit dem Kürzel STP. Nodes prüfen Blöcke und Transaktionen, führen einen gemeinsamen UTXO-Zustand und verbreiten gültige Daten über ein Peer-to-Peer-Netz. Die Chain besitzt einen eigenen Genesis-Block, eigene Adresspräfixe und eigene Netzwerkports. Sie ist kein Token einer anderen Chain und keine Fortsetzung der früheren Python-Versionen von Stompi.

Der Core basiert technisch auf Bitcoin Core v31.1 und nutzt dessen Transaktions- und Blockmodell, secp256k1-Schlüssel, SHA-256d-Proof-of-Work und Bitcoin-artige RPC-Schnittstellen. Stompi-spezifische Parameter und Software müssen separat beurteilt werden. Der Quellcode mitsamt Lizenzhinweisen ist als Paket veröffentlicht.

2. Ziel und Architektur

Selbst prüfen

Eine Person kann eine eigene Node betreiben und dadurch eingehende Blöcke und Transaktionen nach den lokal implementierten Konsensregeln prüfen. Ein Explorer stellt bestätigte Chain-Daten dar; er ersetzt keine eigene Prüfung durch den Empfänger. Wallet-Schlüssel bleiben auf dem jeweiligen Gerät und sind keine Daten des öffentlichen Explorers.

Mining als separater Dienst

Die Stompi-Node bietet Blockvorlagen und Blockannahme über lokalen RPC. Eine separate Python-Brücke stellt Stratum V1 für SHA-256-ASICs bereit. Miner melden sich dort mit einer eigenen Stompi-Adresse an; bei erfolgreichem Solo-Mining zahlt die Coinbase an die angegebene Adresse. Share-Zähler der Brücke sind keine bestätigten Auszahlungen und können bei einem Neustart zurückgesetzt werden.

Netzwerkübersicht

P2P-Port	TCP 28333, für eingehende Peers
RPC-Port	TCP 28332, nur lokal; Cookie privat
Start-Peers	89.163.148.47 · 89.163.242.248 · 91.194.84.84 · 89.163.251.132
Adressformat	Bech32 stp1...; zusätzlich P2PKH stpA... und P2SH stpS...

3. Konsens und Blockerzeugung

Ein Block enthält einen Header mit Vorgänger-Hash, Merkle-Root, Zeitstempel, kompaktem Schwierigkeitsziel und Nonce. Der SHA-256d-Hash des Headers muss das in nBits kodierte Ziel erfüllen. Nodes prüfen zusätzlich unter anderem Transaktionsregeln, Ausgaben und die gültige Verknüpfung mit dem bisherigen Kettenzustand. Die Brücke kann keine Konsensregel ändern; ihr Share-Ziel dient nur der Miner-Kommunikation.

Die Zielblockzeit beträgt 600 Sekunden. Der Sollabstand ist kein Zeitlimit für einzelne Blöcke: Zufall und verfügbare Hashrate können erheblich kürzere oder längere Abstände bewirken. Der Hauptnetz-Code passt die Schwierigkeit alle 2016 Blöcke anhand einer Sollzeitspanne von 14 Tagen an; die Anpassung je Intervall ist begrenzt. Eine Veränderung dieser Regeln wäre eine Konsensänderung, die alle beteiligten Nodes abgestimmt übernehmen müssten.

4. Genesis und Geldmenge

Genesis-Zeit	24. September 2026, 10:00 UTC
Genesis-Hash	000000004ce46ead4546e107fc01668e9f3dafa15452a0766d9a03bc2167917b
Genesis-Bits / Nonce	1d00ffff / 1883639016
Genesis-Text	Stompi 24/Sep/2026: fair launch, no premine

Die anfängliche Subvention beträgt 50 STP je regulärem Block und wird alle 210.000 Blöcke durch ganzzahlige Halbierung reduziert. Die theoretische Ausgabe nähert sich 21 Millionen STP. Der Coinbase-Ausgang des Genesis-Blocks ist nicht ausgebaut. Normale Coinbase-Ausgänge benötigen 100 Blöcke Reife, bevor sie ausgegeben werden können. Transaktionsgebühren kommen zum jeweiligen Blockertrag hinzu und werden von Transaktionen getragen.

Der Text im Genesis-Block dokumentiert die Absicht eines Starts ohne Vorabzuteilung; allein dieser Text beweist keine vollständige unabhängige Prüfung der anfänglichen Verteilung. Für Aussagen zur bereits ausgegebenen Menge zählt die aktuelle, unabhängig überprüfte Chain.

5. Wallets, Transaktionen und Schnittstellen

Stompi verwendet acht Nachkommastellen. Die Standard-Empfangsadresse nutzt das Bech32-Präfix stp und beginnt üblicherweise mit stp1. Weitere unterstützte Formate sind stpA für P2PKH und stpS für P2SH. SegWit ist ab Blockhöhe 1 aktiviert; Taproot ist in den vorliegenden Mainnet-Parametern nicht aktiviert. Betreiber müssen eine Wallet sichern und den Zugriff auf private Schlüssel sowie RPC-Cookie begrenzen.

Eine Zahlung gilt für die Integration erst nach Prüfung der Transaktion in einem Block der eigenen aktiven Chain als bestätigt. Reorganisationen können eine zuvor gesehene Bestätigung zurücknehmen. Die erforderliche Zahl der Bestätigungen ist keine Konstante dieses Whitepapers, sondern muss dem Risiko der jeweiligen Anwendung entsprechen.

6. Betriebsmodell und Freigabepfung

Zum Stand dieser Ausgabe betreibt das Projekt vier bekannte Start-Nodes und eine öffentliche Homepage mit Explorer und Pool-Anzeige. Andere Betreiber können unabhängige Nodes starten und über den P2P-Port verbinden. Vier Projekt-Nodes sind kein Nachweis für vier unabhängige Betreiber oder eine gleichmäßig verteilte Mining-Hashrate.

Im Freigabetest liefen 153 CTest-Gruppen ohne Fehler; eine Gruppe wurde übersprungen. Eine neue Ubuntu-24.04-Node und die Windows-11-GUI synchronisierten und meldeten an geprüften Höhen denselben Blockhash wie die Hauptnode. Eine Übertragung von 0,001 STP wurde mit einem Block bestätigt. Diese Stichproben belegen Funktionsfähigkeit in den getesteten Fällen, kein umfassendes Audit oder eine allgemeine Garantie für Konsenssicherheit.

7. Risiken und offene Arbeiten

Konsens und Reorganisationen

Unabhängige Reviews der Blockprüfung, Schwierigkeitsanpassung, Aktivierungsregeln, Fork-Wahl und schwieriger Reorganisationsfälle stehen aus.

Mining-Konzentration

Bei konzentrierter Hashrate kann die praktische Sicherheit des Netzes deutlich unter einer durch die bloße Zahl von Nodes suggerierten Sicherheit liegen. Die Hashrate sollte fortlaufend und nachvollziehbar beobachtet werden.

Binaries und Updates

Die Archive besitzen veröffentlichte SHA-256-Summen. Bytegleiche unabhängige Reproduktion und eine separat signierte Freigabe sind noch nicht nachgewiesen.

Integration und Betrieb

Börsen und Zahlungsdienste sollten eigene Nodes, Backup- und Wiederanlaufprozesse, Reorg-Erkennung und für ihren Anwendungsfall geeignete Bestätigungsregeln erproben.

8. Technische Quellen und Kontakt

Primärquellen für Parameter und Regeln sind das Stompi-Core-Quellpaket, besonders `src/kernel/chainparams.cpp` (Netzwerk und Genesis), `src/pow.cpp` (Schwierigkeitsanpassung), `src/validation.cpp` (Subvention) und `src/consensus/consensus.h` (Coinbase-Reife). Änderungen an diesen Dateien können eine neue Fassung dieses Dokuments erforderlich machen.

Öffentliche Einstiegspunkte: stompi.tech · [Explorer](#) · [Downloads und Quellcode](#) · [Maschinenlesbares Profil](#). Technischer Kontakt: Thomas@stompi.de.

Dieses Whitepaper ist eine technische Beschreibung, keine Anlageempfehlung und keine Zusage eines Handelsplatzes. Es beschreibt den Stand vom 26. September 2026. Für aktuelle Höhe, Schwierigkeit und aktive Chain sind Live-Daten einer synchronisierten Node maßgeblich.